UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,266	03/30/2000	Vipin Samar	OR99-17401	8991

51067 7590 06/12/2008

PVF -- ORACLE INTERNATIONAL CORPORATION
c/o PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER	
ENGLAND, DAVID E	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
06/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/539,266	SAMAR, VIPIN	
	Examiner	Art Unit	
	DAVID E. ENGLAND	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,10,13,22,25 and 33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,10,13,22,25 and 33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 10, 13, 22, 25 and 33 are presented for examination.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/21/2008 has been entered.

Claim Objections

3. Claims 10, 22 and 33 objected to because of the following informalities: The claims state that the retrieving the running message digest includes authenticating and authorizing the first server, when it appears that with the amended independent claims, the Applicant means Second Server. Applicant is asked to amend this oversight or point to sections of the Specification if this is what the Applicant means. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 10, 13, 22, 25 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abramson et al. (6539494) (hereinafter Abramson) in view of Sandhu et al. (6985953) (hereinafter Sandhu) in further view of RFC 1321.

6. Referencing claim 1, as closely interpreted by the Examiner, Abramson teaches a method for sharing secure communication session, the method comprising:

7. establishing a secure session between a client and a first server, wherein the first server publishes on a backup server a set of session state information for the session, (e.g., col. 4, lines 5 – 39, col. 6, lines 15 – 33), and wherein the session state information includes:

8. an session identifier, (e.g., col. 6, lines 15 – 23);

9. and wherein the first server publishes updates to the session information to the backup server, (e.g., col. 6, lines 15 – 23);

10. receiving a message from the client at a second server, wherein the message includes the session identifier, and wherein the client, the first server, the second server, and the backup server are different from one another, (e.g., Fig. 7);

11. determining that an session corresponding to the received session identifier is not configured on the second server, (e.g., col. 6, lines 15 - 49, The alias server and back up server are used in the migration of a session ID to another server.);

12. querying the database with the received session identifier, (e.g., col. 6, lines 15 - 49);

13. retrieving from the database identifier the session state information which corresponds to the received session identifier and which is published by the first server, (e.g., col. 6, lines 15 - 49);

14. establishing an session between the client and the second server with the same session identifier based on the retrieved session state information, (e.g., col. 6, lines 15 - 49); and

15. using the session identifier to send a second message from the second server to the client through the session without establishing a separate session between the client and the second server, (e.g., col. 6, lines 15 - 49).

16. Abramson does not specifically teach secure socket layer (SSL) session;

17. a database including:

18. a read key for encrypting communications from the client;

19. a write key for encrypting communications from the first server;

20. an encrypted running message digest; and

21. a message digest key which is used to encrypt the running message digest; and

22. wherein the first server continually changes the running message digest as messages are sent through the SSL session, and wherein the first server publishes updates to the running message digest to the database;

23. Although Abramson does teaches multiple servers to store information about session data it would only take one of ordinary skill in the art to implement a specific database in the server to be utilized in storing more information per user since it is known in the art that databases are used to organize and make data more efficient available to the system.

24. Sandhu teaches secure socket layer (SSL) session between multiple nodes, (e.g., col. 6, lines 20 – 35);

25. storing:

26. a read key for encrypting communications from the client, (e.g., col. 9, lines 12 – 40);

27. a write key for encrypting communications from the first server, (e.g., col. 9, lines 12 – 40);

28. an encrypted running message digest, (e.g., col. 9, lines 12 – 40); and

29. a message digest key which is used to encrypt the running message digest, (e.g., col. 9, lines 12 – 40); and

30. wherein the first server continually changes the running message digest as messages are sent through the SSL session, (e.g., col. 9, lines 12 – 40, It is known in the art that if the data that is put through a message digest algorithm is changed, the message digest is also changed for that data and therefore the updates to the cookie that are taught would change the message digest, see RFC 1321 below.).

31. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Sandhu with Abramson because utilizing a running message digest allows for a different string to be produced every time the algorithm is run, therefore, giving more security to a system and having less of a opportunity for intruders to duplicate the message. Although, Sandhu does not specifically teach wherein the first server continually changes the running message digest as messages are sent through the SSL session, Sandhu teaches MD5. As seen in RFC 1321, MD5 is a running message digest that is always changing and therefore RFC 1321 teaches continually changes a running message digest as messages are sent through the

secure communication session, (e.g., pages 1 – 9). It would have been obvious to one of ordinary skill in the art to utilize MD5 for secure communication because it is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.

32. As per claim 10, Abramson does not teach retrieving the running message digest includes authenticating and authorizing the first server.

33. Sandhu teaches retrieving the state information includes authenticating and authorizing the first server, (e.g., col. 9, lines 11 – 40 & col. 12, lines 25 - 52). It would have been obvious to one skilled in the art at the time the invention was made to combine Sandhu with Abramson because it would make a system more secure if the receiver of the information could be authorized to the information by authenticating the information that was sent from the first server and for similar reasons stated above

34. The teachings for claims 13, 22, 25 and 33 can be found in the same areas as stated in the above claims and therefore are rejected for similar reasons as stated above.

Response to Arguments

35. Applicant's arguments filed 03/21/2008 have been fully considered but they are not persuasive.

36. In the Remarks, Applicant argues in substance that Abramson, Sandhu and RFC 1321 do not teach the amended claims.

37. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

38. **Applicant is invited to contact the Examiner again to aid in furthering prosecution and coming to an agreement to the claim language.**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DAVID E. ENGLAND whose telephone number is (571)272-3912. The examiner can normally be reached on Mon-Thur, 7:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan J. Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

David E. England
Primary Examiner
Art Unit 2143

/David E. England/
Primary Examiner, Art Unit 2143